

REMARKS

I. INTRODUCTION

In response to the Office Action dated March 22, 2004, no claims have been amended. Claims 1-17 remain in the application.

II. CLAIM AMENDMENTS

Applicants' attorney has made amendments to the claims as indicated above. These amendments were made solely for the purpose of clarifying the language of the claims, and were not required for purposes of patentability.

III. STATUS OF CLAIMS

Claims 1-17 were rejected under 35 U.S.C. §102(e) as being anticipated by Rallis et al., U.S. Patent No. 6,425,084 (Rallis).

IV. STATUS OF AMENDMENTS

No amendments to the claims have been made subsequent to the final Office Action.

V. ISSUES PRESENTED FOR REVIEW

Whether claims 1-17 are patentable under 35 U.S.C. § 102(e) over U.S. Patent No. 6,425,084, issued to Rallis et al. (hereinafter, "the Rallis reference", or "Rallis").

VI. ARGUMENTS

A. The Independent Claims Are Patentable Over The Prior Art

1. The Rallis Reference

U.S. Patent No. 6,425,084, issued July 23, 2002 to Rallis et al. discloses a notebook security system using infrared key. An IR key device carries a first serial number and an encryption key. A second serial number corresponds to a device internal to the computer. A mass storage device installed in the computer stores a validation record that includes an unencrypted portion and an encrypted portion, the unencrypted portion including a copy of the first serial number and the

encrypted portion including a copy of said second serial number and a user personal identification number. The key device is coupled and interfaced with an infrared port on the computer by the user. The first serial number and the encryption key are read from the key device in order to gain authorized use of the computer. The key device may be decoupled from the computer after authorized use of the computer has been gained, and during operation of the computer.

2. Claims 1-17 are Patentable Over the Rallis Reference

With Respect to Claims 1 and 4: Claim 1 recites an input device for securing a token from an unauthorized user. The token comprises:

a user interface for accepting entry of a personal identifier from a user;
a processor, communicatively coupled to the user interface;
a token interface, including:
a token interface emitter, for producing a signal having information including the personal identifier, the token interface emitter communicatively coupled to the processor and further communicatively coupled to a token sensor when the token is physically coupled with the token interface; and
a shield, substantially opaque to the signal, for substantially confining reception of the signal to the token sensor.

Both the First and Final Office Actions assert that Rallis discloses an input device for securing a token from an unauthorized user:

“Second, the Rallis reference discloses that the user must enter the pin in order to be validated (see col. 1, lines 61-65, col. 2, lines 59-67). Therefore, Rallis does disclose an input device for securing a token from an unauthorized user.”

This is incorrect. Rallis discloses an input device (e.g. keyboard 46). But the purpose of Rallis is to secure a computer from unauthorized use. That is accomplished using an input device and a token, but that does not mean that the input device secures the *token* from unauthorized use.

With regard to the Final Office Action's further arguments, the Applicants invite consideration of FIG. 6E, which is reproduced and described below in modified form. The Applicants respectfully submit that of all that is disclosed in the Rallis reference, FIG. 6E comes closest to what might rationally be considered to read on claim 1.

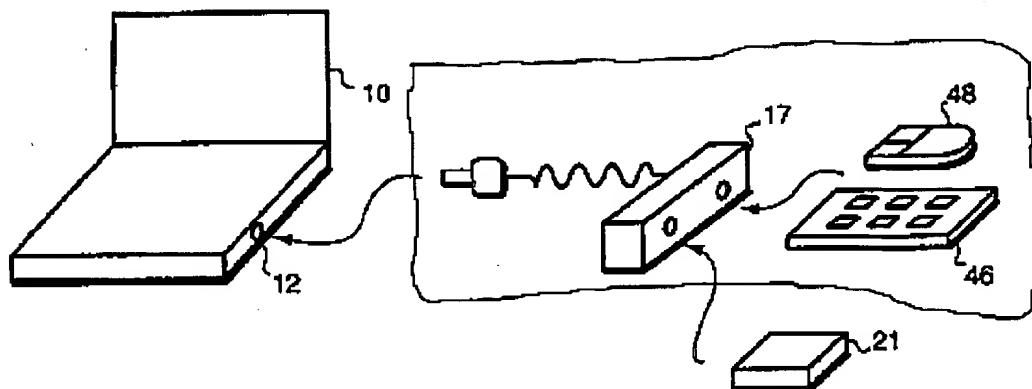


FIG. 6E

In another alternative, a PS-2/IR "Y" connector 17, equipped with an internal automatic switch (not shown), is employed to permit the simultaneous IR connection of an IR key device 21 and a keyboard 46 (or mouse 48) to a notebook computer 10 as shown in FIG. 6E. (col. 6, lines 21-25)

One might be tempted to regard the circled portion of FIG. 6E to be the "input device" recited in claim 1. But if one were to argue that "user interface" reads on the keyboard 46, the "processor" reads on a processor inside the "Y" connector 17, and the "token interface emitter" reads on the output of the "Y" connector (on the left margin of the drawn line), the features of claim 1 are still not disclosed, because the "token interface emitter" is not coupled to the "token sensor" (which would presumably be included in 21).

Similarly, if one were to argue that the "token interface emitter" were the interface between the "Y" connector 17 and the token 21, the "token interface emitter" would not produce a signal having the personal identifier as recited in claim 1 (the PIN is not transmitted to the token 21).

The Final Office Action continues to allege that the PIN is transmitted to the token, relying on the following passage:

60 Ideally, the key device 20 is of such shape and size as to be placed on the user's key chain. It receives power and command messages from the notebook computer 10 and returns response messages, a serial number and an encryption key. A program running on the notebook computer 10 uses the key device serial number and the encryption key, along with a Personal Identification Number (PIN), in a
65 user-validation procedure to prevent operation (i.e. power-up) of the note book computer 10 by an unauthorized user.

Nothing in the foregoing teaches transmitting the PIN to the token. On its face, it merely says that the program *uses* a PIN.

Finally, as the Applicants have pointed out, nothing in Rallis even remotely suggests a "shield", and in fact, Rallis teaches away from the use of a "shield".

The First Office Action relied upon the following passage to allege that a shield was disclosed:

When prompted by the user-validation program, the user aligns the IR key device 21 with the IR port 16 and depresses the switch 25 within the allotted time period (e.g. 30 seconds). The IR key device 21 transmits a message that includes the key device serial number and the encryption key using the Ultra Protocol as established by the Infrared Data Association (IrDA). (col. 5, lines 51-57)

And the Final Office Action relied on the following:

The key device driver 112 provides the application interface to the key device 20. It reads the key device serial number and the encryption key, matches the key device serial number to that of the validation record stored on the hard disk, and uses the encryption key to decrypt the encrypted portion of the validation record. (col. 6, lines 63-68)

Of course, none of the foregoing discloses a shield or any analogous structure. The Final Office Action appears to argue that the use of an encryption key and a decryption key constitutes a "shield":

"The Examiner disagrees with the Applicant, because Rallis discloses an encryption key that must have a corresponding decryption key in order to validate."

Even if a decryption key and an encryption key could rationally be interpreted as a "shield" (and it cannot), it cannot possibly read on the claimed feature "substantially opaque to the signal, for substantially confining reception of the signal to the token sensor."

Accordingly, the Applicants traverse the rejection of claim 1.

With Respect to Claim 2: Claim 2 recites that the token interface emitter is communicatively decoupled from the token sensor when the token is not physically coupled to the interface.

According to the First Office Action, this feature is disclosed as follows:

A flow diagram of the user-validation procedure is shown in FIG. 3. In Step 1, the user-validation program prompts the user to attach the key device 20 to the notebook computer 10. The program attempts to communicate with the key device 20 for a fixed delay period. If a key device 20 is not detected within this period, then the program proceeds to Step 11 where the computer is automatically powered down. (col. 3, lines 18-24).

According to the Final Office Action, this feature is disclosed as follows:

In an alternative interface, the IR key device 21 is equipped for Infrared (IR) communications with a notebook computer 10 via the IR port 16 as shown in FIG. 6A. Ideally, the IR key device 21 is of such shape and size as to be placed on the user's key chain. It is self-powered and in its basic configuration, as shown in FIG. 6B, includes an IR transmitter 27 and a momentary transmit switch 25, in addition to a microprocessor and ROM (not shown). When prompted by the user-validation program, the user aligns the IR key device 21 with the IR port 16 and depresses the switch 25 within the allotted time period (e.g. 30 seconds). (col. 5, lines 44-54)

The Applicants respectfully disagree. Rallis teaches a key that is communicatively coupled to the laptop computer, even when the two are not physically coupled. Hence, Rallis not only fails to disclose the features of claim 2, it teaches away from these features.

With Respect to Claim 4: Claim 4 recites that the shield substantially circumscribes the token interface emitter. This feature is not disclosed in the Rallis reference, and therefore, claim 4 is allowable as well.

Although the Applicants traversed the rejection of claim 4, the Final Office Action does not provide further guidance regarding the rationale for this rejection. The Applicants respectfully request that this issue be addressed in the Advisory Action.

With Respect to Claim 5: Claim 5 recites that the token interface comprises "*a token interface sensor configured to receive the signal produced by a token emitter when the token is physically coupled with the token interface*". According to the Office Action, this feature is described as follows.

When prompted by the user-validation program, the user aligns the IR key device 21 with the IR port 16 and depresses the switch 25 within the allotted time period (e.g. 30 seconds). The IR key device 21 transmits a message that includes the key device serial number and the encryption key using the Ultra Protocol as established by the Infrared Data Association (IrDA). (col. 5, lines 51-57)

The Applicants respectfully disagreed. The IR embodiment of the Rallis reference (the only embodiment could be interpreted to disclose a token emitter) is disclosed as an alternative embodiment, not one that is used in conjunction with the embodiment using the USB or PS/2 port. Hence, the Rallis reference fails to disclose or suggest the features recited in claim 5, and claim 5 is allowable.

The Final Office Action did not further address the rejection of claim 5. The Applicants respectfully request that this issue be addressed in the Advisory Action.

With Respect to Claims 6 and 7: Claim 6 recites that the token emitter emits a second signal including information describing the intensity of the signal. The First Office Action acknowledges that feature is not explicitly disclosed in the Rallis reference, but relying on the text reproduced below, argues "when the user has a sensor that is an IR signal, and then the signal transmits the intensity, because the sensor senses when the user is in a certain range".

When prompted by the user-validation program, the user aligns the IR key device 21 with the IR port 16 and depresses the switch 25 within the allotted time period (e.g. 30 seconds). The IR key device 21 transmits a message that includes the key device serial number and the encryption key using the Ultra Protocol as established by the Infrared Data Association (IrDA). (col. 5, lines 51-57)

and

In the "super key" configuration, the IR key device 21 includes both an IR transmitter and IR receiver, but does not include a transmit switch. The IR key device 21 remains the powered-down state until it receives an IR pulse. (col. 6, lines 7-10)

This, of course, does not disclose a *token emitter* transmitting a *second signal* having information describing the intensity of the (first) signal.

The Final Office Action argues that Rallis "discloses the intensity of the signal, key device sends commands low nibble and high nibble."

The Applicants do not understand the relevance of "low nibble" and "high nibble" to claim 6, and therefore traverse this rejection.

With Respect to Claim 7: Claim 7 recites that the processor controls the intensity of the first signal according to the information describing intensity of the first signal received from the second signal. The Final Office Action claims that Rallis inherently discloses this feature, because "Rallis waits for the command from the processor."

Waiting for a command does not read on the features of claim 7. Accordingly, the Applicants traverse the rejection of claim 7.

With Respect to Claim 8: Claim 8 recites:

transmitting the user-entered personal identifier to the token via a communication path distinct from the USB-compliant interface.

According to the First Office Action, the Rallis reference discloses the step of transmitting the user-entered personal identifier to the token via a communication path distinct from the USB-compliant interface as follows:

When prompted by the user-validation program, the user aligns the IR key device 21 with the IR port 16 and depresses the switch 25 within the allotted time period (e.g. 30 seconds). The IR key device 21 transmits a message that includes the key device serial number and the encryption key using the Ultra Protocol as established by the Infrared Data Association (IrDA). (col. 5, lines 51-57)

The Final Office Action offered no further guidance regarding this rejection.

Clearly, Rallis does not disclose transmitting the user entered PIN to the token. The Rallis reference does not disclose transmitting a PIN to the token at all, and in fact, teaches away from doing so. The Applicants therefore traverse this rejection.

With Respect to Claims 9 and 10: Claims 9 and 10 are allowable for the same reasons as claim 8.

With Respect to Claim 11: Claim 11 recites that the signal is shielded to confine reception of the signal to the sensor. This claim is allowable for the same reasons described with respect to claim 1 above.

With Respect to Claims 12-14: Claims 12 and 13 are allowable for the same reasons as claim 8. Further, nothing in the Rallis reference discloses determining if a token is accepted by sensing a connect signal.

With Respect to Claim 15: Claim 15 recites that the step of determining if the token has been accepted by the input device comprises the step of receiving a second signal produced by the token emitter after the token sensor receives a third signal in the token interface. According to the Office Action, these features are disclosed in the Rallis reference as follows:

The procedure permits entry past a first security level only if the key device serial number matches the unencrypted numbers in the validation record. If the first-level validation is successful, the procedure then uses the encryption key to decrypt the hard drive serial number and PIN found in the stored validation record. The procedure permits entry past the second security level only if the validation record is properly decrypted, the installed hard disk serial number matches the decrypted number, and the manually-entered PIN matches the decrypted PIN. A failure at any step in the user-validation procedure will immediately power down the computer, thereby rendering it useless to a thief not possessing the required key device. (col. 1, line 64, through col. 2, line 10).

According to the First and Final Office Action, the "third signal" is the user's "PIN that is incorrect." The Applicants respectfully traverse. The foregoing is completely unrelated to the subject of claim 15 (determining if the token has been accepted by the input device). Further, the user's PIN is not a signal produced by a token emitter or received by a token emitter.

The Final Office Action provided no further guidance regarding this rejection

With Respect to Claim 16: Claim 16 is allowable for the same reasons as claim 7.

With Respect to Claim 17: Claim 17 recites the step of "*disabling the transmission of the user-entered personal identifier until detection of the acceptance of the token to the USB port.*" The First Office Action indicates that these features are disclosed in Rallis as follows:

For maximum security protection, the key device 20 is connected only during the user-validation procedure and is carried and stored separately from the notebook computer 10. (col. 2, line 67 through col. 3, lines 3)

A flow diagram of the user-validation procedure is shown in FIG. 3. In Step 1, the user-validation program prompts the user to attach the key device 20 to the notebook computer 10. The program attempts to communicate with the key device 20 for a fixed delay period. If a key device 20 is not detected within this period, then the program proceeds to Step 11 where the computer is automatically powered down. (col. 3 and 18-24)

The Applicants do not understand where the foregoing passages disclose disabling the

transmission of a user-entered personal identifier until detection of the acceptance of the token to the USB port. Rallis, in fact, does not teach transmitting a PIN anywhere, and certainly does not teach disabling transmission of a user-entered PIN until a token is accepted into a USB port.

The Final Office Action responds:

"Rallis does disclose disabling the transmission of the user-entered Pin until detection of the token to the port, because if the key device is not detected the computer is powered down, and thus the messages of the pin transmitted cannot be transmitted"

The Applicants do not understand the meaning of this statement, and respectfully traverse the rejection of claim 17.

VII. CONCLUSION

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.


Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicant(s)

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: May 24, 2004

VGC/io

By: 
Name: Victor G. Cooper
Reg. No.: 39,641